IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

MÖLNLYCKE HEALTH CARE US, LLC, Plaintiff, v. WILLIAM PURDY, ROBERT PURDY, AND GREENWOOD MARKETING, LLC Defendants.	Civil Action No. 7:20-cv-03755 (CS)
WILLIAM PURDY, ROBERT PURDY, AND GREENWOOD MARKETING, LLC Counterclaim-Plaintiffs, v. MÖLNLYCKE HEALTH CARE US, LLC, Counterclaim-Defendant.	

[PROPOSED] ESI DISCOVERY ORDER

Upon consideration of the Parties' Joint Motion for Entry of an ESI Discovery Order, it is hereby ORDERED as follows:

1. The Parties hereby agree to the following protocol for production of electronically stored information ("ESI") and paper ("hardcopy") documents. Subject to protective orders in this Action, this order governs all production in this matter. It streamlines the production of ESI and hardcopy documents to promote a "just, speedy, and inexpensive determination" of this Action, including any disputes pertaining to scope or costs, as required by Federal Rule of Civil Procedure 1.

2. Nothing in this protocol shall limit a Party's right to seek or object to discovery based upon applicable local rules or federal civil rules of procedure, to rely on any protective order entered in this Action concerning protection of confidential or otherwise sensitive information, to assert attorney-client or other applicable privileges as a basis to withhold disclosure, or to object to the authenticity or admissibility of any hardcopy document or ESI produced in accordance with this protocol. The mere production of ESI as part of a mass production shall not itself constitute a waiver for any purpose.
3. This Order may be modified in the Court's discretion or by agreement of the Parties. If the Parties cannot resolve disagreements regarding modifications, the Parties shall submit their competing proposals and a summary of their dispute to the Court.
4. Upon application to the Court, after reasonable efforts among counsel to resolve their disputes and streamline discovery through the "meet and confer" process, costs may be shifted for disproportionate ESI production requests pursuant to Federal Rule of Civil Procedure 26. Likewise, a Party's nonresponsive or dilatory discovery tactics will be cost-shifting considerations. A Party's meaningful compliance with this Order and efforts to promote efficiency and reduce costs will be considered in cost-shifting determinations.
5. In its productions of ESI in this case, the Parties agree to use the form of production set out in Appendices A and B to this Order, which shall be deemed to be production in reasonably usable form under Rule 34.
6. The Parties are aware of the importance the Court places on cooperation and commit to continue to consult and cooperate reasonably as discovery proceeds.
7. The proportionality standard set forth in FRCP Rule 26(b)(1) shall apply to discovery in this Action. Consistent with that proportionality standard, the Parties agree to cooperate

in identifying appropriate limits on discovery, including phased discovery and limits on the number of custodians, on discoverable data sources, on the relevant period, and on the permissible scope of requests for production, in particular, the permissible scope of requests for emails. Requests for production of ESI, including requests for emails, shall be reasonably targeted, clear, and as specific as possible, rather than general discovery of a product or business.

8. **Email Production Requests.** The following provisions shall govern discovery of email in this action:

   a. Consistent with the proportionality standard, the parties agree to engage through counsel in a cooperative, "meet and confer" process designed to facilitate the search and production of emails in a manner that is cost-effective, prompt, and reasonably designed to capture and produce information potentially relevant to the parties' claims, defenses and counterclaims.

   b. The first phase of this process will require the parties to identify likely custodians of potentially relevant information. Within seven (7) days after execution of this proposed order by counsel, each Party shall provide to the other Parties a list of the Party's or Parties' (in the case of Defendants) twelve (12) most likely custodians of documents and information related to the claims, defenses, and counterclaims asserted in this action, as well as a list of non-custodial data repositories or identification of classes of repositories, whose reasonably accessible ESI, including emails as appropriate, will be searched for relevant information. Custodians shall be identified by name, current or last title, dates of

employment by the Party, and a brief description of current or last employment duties.

c. When providing a list of likely custodians, the Party or Parties providing the list shall also indicate whether and to what extent each custodian's ESI, including but not limited to emails, hard drives, or other data repositories, have been preserved and are reasonably accessible for purposes of conducting a search. If any custodian identified by either Party (and/or the ESI associated with that custodian) is located outside the United States, the Parties shall meet and confer regarding such matters as relevancy and privacy of the data at issue and, as applicable, the timing of production of any such data.

d. Within seven (7) days after identifying likely custodians, the parties shall meet and confer to identify and agree upon an email search and production protocol, identifying the proper custodians, proper search terms and proper timeframe for search and production of emails and associated ESI responsive to their respective document demands ("the Email Requests").

f. In connection with such search and production protocols, and except as provided herein, by agreement among counsel, or with Court approval, each party shall limit its Email Requests to a total of eight (8) custodians per Producing Party for all such requests. The Parties may jointly agree to modify this limit without the Court's leave. In the event the Parties cannot agree to such modification, the Court shall consider contested requests for searches involving additional custodians, upon the Requesting Party's showing of a distinct need based on the size, complexity, and issues of this specific case.

g. Each Requesting Party shall limit its Email Requests to a total of ten (10) searches per custodian. If the Requesting Party wishes to run a lesser number of searches for one or more custodians, he/she/it may elect to apply the unused searches to another custodian, from whom additional searches are sought beyond ten (10). (By way of example only, if Requesting Party seeks to run only six searches as to custodian A, Requesting Party may request that fourteen (14) searches be run as to custodian B.) The Parties may jointly agree to modify the above-described limits on searches without the Court's leave. In the event the Parties cannot agree to such modification, the Court shall consider contested requests for additional search terms, upon the Requesting Party's showing of a distinct need based on the size, complexity, and issues of this specific case.

h. Where practicable, the search terms or phrases shall be narrowly tailored to particular issues. Indiscriminate terms, such as the producing company's name or its product name, may be inappropriate unless combined with narrowing search criteria that sufficiently reduce the risk of overproduction. A conjunctive combination of multiple words or phrases (e.g., "computer" and "system") narrows the search and shall count as a single search term. A disjunctive combination of multiple words or phrases (e.g., "computer" or "system") broadens the search, and thus each word or phrase shall count as a separate search term, unless they are variants of the same word (e.g., "dog" or "canine"). Use of narrowing search criteria (e.g., "and," "but not," "w/x") is encouraged to limit the production and associated burdens and expenses.

i. To the extent that one or more Email Requests propounded by a Party yields an unreasonable amount of "hits" (search results containing the search term or phrase), such that review and production of same may be viewed as unduly burdensome and expensive, the Producing Party shall promptly so notify the Requesting Party and identify the custodian, the specific Email Request objected to, and the number of hits that the Email Request yielded. In that event, the parties agree to "meet and confer" promptly and engage in a cooperative, iterative effort to refine the search terms and thereby narrow the resulting hits to a more manageable number. Such efforts at refining search terms to and narrow search results shall be encouraged, for the benefit of both parties, and the resulting searches shall not be viewed as "new" or "additional" Email Requests, for purposes of the agreed-upon search limits identified in paragraph (g) above. If, but only if, the parties are unable to agree upon what constitutes a reasonable number of hits and/or a properly refined search term or phrase, they shall submit their dispute to the Court for a ruling.

j. Within seven days after the Parties have identified their custodians and search terms, each Party shall run their searches, and all resulting responsive, non-privileged ESI documents shall be produced on a rolling basis as soon as practicable thereafter – with such production to be substantially completed within 30 days after the search terms are finalized.

9. **Discovery Concerning Preservation and Collection Efforts.** Discovery concerning the preservation and collection efforts of another Party can contribute to unnecessary expense and delay and may inappropriately implicate work product and attorney-client privileged

matter. If there is a reasonable question or dispute concerning the scope of a Party's preservation or collection efforts, the Parties or their counsel must meet and confer and fully explain their reasons for believing that additional efforts are, or are not, relevant and proportional pursuant to Rule 26(b)(1). In particular, before serving demands for document discovery about preservation and collection, a Party shall confer with the other Party concerning the specific need for such discovery, including its relevance to claims and defenses, its proportionality to the needs of the case, and the suitability of alternative means for obtaining the information. Notwithstanding the foregoing, the parties are free to seek basic information about a Party's preservation and collection efforts by means of questions posed at deposition or through written interrogatories.

10. **On-Site Inspections of ESI**. On-site inspections of ESI under Rule 34(b) shall be permitted only upon a good faith showing by the Requesting Party of good cause and specific need, as determined by the Court, or upon agreement of the Parties. As appropriate, the Court may condition on-site inspections of ESI, as authorized in the preceding sentence, to be performed by independent third-party experts, and the Court may set other conditions deemed appropriate by the Court.

11. **Non-Discoverable ESI.** Consistent with the proportionality standard, and absent a Party's specific written notice for good cause (which shall be determined by agreement or upon application to the Court), the following categories of ESI are generally presumed to be inaccessible and not discoverable absent good cause shown:

    a. ESI deleted in the normal course of business before the time a preservation obligation in this matter arose (including but not limited to the duty to preserve

documents and other information potentially relevant to the claims, counterclaims and defenses in this action);

b. Backup data files that are both: (i) maintained in the normal course of business for purposes of disaster recovery, including (but not limited to) backup tapes, disks, SAN, and other forms of media, and (ii) substantially duplicative of data that are more accessible elsewhere;

c. Deleted, "slack," fragmented, or unallocated data only accessible by forensics;

d. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;

e. On-line access data such as (without limitation) temporary internet files, history files, cache files, and cookies;

f. Data in metadata fields frequently updated automatically, such as last-opened or last-printed dates;

g. Electronic data (e.g., call logs, email, calendars, contact data, notes, etc.) sent to or from mobile devices (e.g., iPhone, iPad, Android, and Blackberry devices), if a copy of such electronic data is routinely saved elsewhere and is more accessible in that latter format (such as on a server, laptop, desktop computer, or 'cloud' storage). For the avoidance of doubt, should a Party make use of applications on mobile devices for inventory tracking, purchasing, location of equipment, or the like, not only is the data input by the party into the application deemed discoverable ESI, so would be the application itself. This provision does not limit a Party's ability to object to production of any such data or application on any basis, including without limitation relevance, proportionality, or undue burden.

g. Voicemail, including Telephone or VOIP voice messages that (i) are not retained in the ordinary course of business; and (ii) were deleted or rendered not reasonably accessible before the time a preservation obligation in this matter arose (including but not limited to the duty to preserve documents and other information potentially relevant to the claims, counterclaims and defenses in this action);

h. Text messages and instant messages that (i) are not retained in the ordinary course of business; and (ii) were deleted or rendered not reasonably accessible before the time a preservation obligation in this matter arose (including but not limited to the duty to preserve documents and other information potentially relevant to the claims, counterclaims and defenses in this action);

i. Server, system, network, or software application logs;

j. Data remaining from systems no longer in use that is unintelligible on the systems in use, except to the extent that the changeover to a new system occurred during the period that the Party had a preservation obligation in this matter (including but not limited to the duty to preserve documents and other information potentially relevant to the claims, counterclaims, and defenses in this action);

k. Electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data is not ordinarily preserved as part of a laboratory report;

l. Files included on the National Institute of Standards and Technology (NIST) modern RDS (minimal) list, available at https://www.nist.gov/itl/ssd/software-quality-group/nsrl-download/current-rds-hash-sets;

m. Structural files not material to legibility of individual file contents (e.g., CSS, .XSL, .XML, .DTD, etc.);

n. Operating System files that do not store user-created content (e.g., CAT, DLL, DMP, EXE, FON, PNF, OPS, SYS, etc.);

o. Application source code, configuration, and other similar files necessary for the function of an application that do not store user-created content during ordinary use (E.g. BAK, BIN, CFG, DBF, DAT, JS, JSON, JAR, LUA, MSB, RES, WINNT, YTR etc.)

12. **Disaster-Recovery Backup Data.** Consistent with the proportionality standard, and absent a Party's specific written notice for good cause, no Party shall be required to modify or suspend procedures, including rotation of backup media, used in the normal course of business to back up data and systems for disaster recovery purposes. Absent a showing of good cause, such backup media shall be considered to be not reasonably accessible.

13. **No Designation of Discovery Requests.** Productions of hardcopy documents and ESI in the reasonably usable form set out in this protocol, including Appendices A and B, need not be organized and labeled to correspond to the categories in the requests. This provision is inapplicable to any obligations that may exist regarding interrogatory responses that make use of Rule 33(d) of the Federal Rules of Civil Procedure.

14. **Unintentional Production of Privileged Material**. The unintentional production of any material constituting or containing attorney-client privileged information or work-product, or constituting or containing information protected by applicable privacy laws or regulations, shall be governed by provisions contained in the Protective Order entered in

this Action. The Receiving Party shall not use ESI that the Producing Party asserts is attorney-client privileged or work product protected to challenge the privilege or protection; however, the Receiving Party may request that the Court examine such ESI *in camera* to assess the validity of the claimed privilege or protection. Pursuant to Federal Rule of Evidence 502(d), the inadvertent production of a privileged or work product protected ESI is not necessarily a waiver in the pending case or in any other federal or state proceeding. The mere production of ESI in a litigation as part of a mass production shall not itself constitute a waiver for any purpose unless that production forfeits the protections under Federal Rule of Evidence 502.

15. The Parties agree that, should a Party produce documents that exist in the normal course of business only in hard-copy form by scanning and producing them, redacted as necessary, in accordance with the procedures set out in Appendices A and B, such scanned images shall not be treated as ESI.

SO ORDERED.

Cathy Seibel

CATHY SEIBEL, U.S.D.J. 11/30/30

APPENDIX A

Consistent with Paragraph 5 of the [Proposed] ESI Discovery Order ("the Order"), the Parties agree that the production of ESI in the manner set forth below be deemed production in a reasonably usable form.

1. Except as stated in Paragraphs 4 and 5 below or as agreed by the Parties, the Parties may produce documents in single-page TIFF-image or PDF format with extracted or OCR text and the associated metadata set out in Appendix B ("TIFF-Plus format" or "PDF-Plus format").

2. The Receiving Party may seek production in native format of specifically identified ESI produced originally in TIFF-Plus format or PDF-Plus format, for good cause explained in the request. The Producing Party shall respond reasonably and in good faith to any such request. Procedures for production of a native file in response to any such request are set out in Appendix B, Paragraph A.14.b.

3. To the extent that a document or record exists in color, as it is maintained in the normal course of business, it shall be produced in color.

4. Native Files. Discoverable portions of electronic spreadsheets (e.g., Excel), electronic presentations (e.g., PowerPoint), word processing files with tracked changes, comments, or hidden text (e.g., Word), desktop databases (e.g., Access), and audio/video multimedia files may be produced in native format as described in Paragraph A.14.a of Appendix B.

5. Enterprise Databases, Database Management Systems, and Other Structured Data ("Structured Data Systems")

a. If discoverable data from Structured Data Systems can be produced in an already existing and reasonably available report, the Producing Party may collect and produce the data in that report format in accordance with Paragraph 1;

b. If an existing report form is not reasonably available, the Producing Party may make reasonable efforts to export from the Structured Data System discoverable information in a format compatible with Microsoft Excel or Microsoft Access and may produce such information in that native format. If reports are generated, the Producing Party agrees to their admissibility under Federal Rule of Evidence 1006.

6. Redactions.

a. The Producing Party may redact from any PDF or TIFF image, metadata field, or native file material that is protected from disclosure by applicable privilege or immunity, or that is required to be redacted by law or regulation, or that the Protective Order entered in this Action allows to be redacted. In preparing document families for production, the Producing Party also may withhold entire attachments that are wholly non-responsive but will produce slipsheets in their place. In that event, the Requesting Party reserves the right to demand production of the full document, with attachments, and such documents must then be produced by the Producing Party, subject only to claims of applicable privilege or immunity.

b. Each redaction in a PDF or TIFF-image should be indicated clearly. When a PDF or TIFF-image is redacted for attorney-client privilege, work-product immunity, or as required by law, the redaction should identify the basis for the redaction unless same is obvious from the face of the document itself.

c. For native files requiring redaction, redacted text may be replaced, when feasible, with the term "Redacted" or, for portions withheld on the grounds of attorney-client privilege or work-product immunity, "Privilege," and the Producing Party shall produce the redacted file either in the reasonably usable form set out in Paragraph 1.a or in native format.

d. If the Receiving Party should challenge any redaction, the Parties shall abide by the terms of the Protective Order and shall handle any such challenge in accordance with those terms.

7. Email Threading.

a. Email threads are email communications that contain lesser-included email communications that also may exist separately in the Party's electronic document collection. A most-inclusive email is one that contains unique content and all the lesser-included emails, including attachments, for that branch of the email thread. The Parties agree that removal of available lesser-included emails from potential production will reduce all Parties' costs of document review, production, and litigation-support hosting, and the parties need not produce such lesser-included emails. Additionally, a Party may produce or list on any required privilege log only the most inclusive email threads.

b. Following production of most inclusive email threads and any privilege logs, and for good cause, a Receiving Party may make reasonable requests for individual lesser-included emails or for more information about privilege log entries regarding email threads. The Producing Party shall cooperate reasonably in responding to any such requests if the requested lesser-included emails otherwise would have been subject to production.

8. Avoidance of Duplicate Production.

a. "Duplicate ESI" means files that are exact duplicates based on the files' MD5 or SHA-1 hash values. The Producing Party need produce only a single copy of responsive Duplicate ESI. A Producing Party may take reasonable steps to de-duplicate ESI globally (i.e., both within a particular custodian's files and across all custodians). Entire document families may constitute Duplicate ESI. De-duplication should not break apart families. When the same Duplicate ESI exists in the files of multiple custodians, those persons may be listed in the OTHER_CUSTODIANS field identified in Paragraph A.13.c of Appendix B.

APPENDIX B

A.1. Image Files. Files produced in PDF format or *.tif format will be single page black and white PDF images or *.tif images at 300 DPI, Group IV compression. Embedded images will not be reduced or below 300 DPI. To the extent possible, original orientation will be maintained (i.e., portrait-to-portrait and landscape-to-landscape). Each PDF or *.tif image will be assigned a unique name matching the production number of the corresponding page. Such files will be grouped in folders of no more than 1,000 *.tif files each unless necessary to prevent a file from splitting across folders. Files may be split across folders and will be mapped accordingly on the .opt file, such that the receiving party can use the .opt file to upload the unitized files. If a file, *e.g.*, a PDF file, exceeds 500 PDF or *.tif images, the producing party may produce the file natively rather than in PDF or *.tif format. Separate folders will not be created for each file. Production ("Bates") numbers shall be endorsed on the bottom of all images. This number shall be a unique, consistently formatted identifier that will:

a. be consistent across the production;

b. contain no special characters; and

c. be numerically sequential within a given file.

Bates numbers should be a combination of an alpha prefix along with a number (e.g. ABC00000001). The number of digits in the numeric portion of the Bates number format should not change in subsequent productions. Confidentiality designations, if any, will be endorsed on the bottom of all images and should not obscure any portion of the original file, unless this is unavoidable.

A.2. File Text. Except where a file's full text cannot be extracted (*e.g.*, when a file has been redacted under assertion of privilege or other protection from disclosure), full text will be provided in the format of a single *.txt file for each file (*i.e.*, not one *.txt file per *.tif image).

Where ESI contains text that cannot be extracted, the available *.tif image will be OCR'd or, as applicable, the redacted native file will have its text re-extracted, and file-level text will be provided. Searchable text will be produced as file-level multi-page UTF-8 text files with the text file named to match the beginning production number of the file. The full path of the text file must be provided in the *.dat data load file. The text file shall include interlineated image keys/bates numbers sufficient to show, for all PDF or TIFF-image pages, the bates-numbered page of the associated text.

A.3. Word Processing Files. If word processing files, including without limitation Microsoft Word files (*.doc and *.docx), are produced in *.tif image format, such *.tif images will display tracked changes, comments, and hidden text. The produced images shall reflect the native files as they were processed, including the files' settings as they were saved to the file before upload. Native files for all file extensions, with the exception of email messages, are to be included in the production, allowing the receiving party to view and/or download the native files for identification of any hidden data, tracked changes, comments or notes.

A.4. Presentation Files. If presentation files, including without limitation Microsoft PowerPoint files (*.ppt and *.pptx), are produced in *.tif image format, such *.tif images will display comments, hidden slides, speakers' notes, and similar data in such files. The produced images shall reflect the native files as they were processed, including the files' settings as they were saved to the file before upload. Native files for all file extensions, with the exception of email messages, are to be included in the production, allowing the receiving party to view and/or download the native files for identification of any hidden data, tracked changes, comments or notes.

A.5. Spreadsheet or Worksheet Files. If spreadsheet files, including without limitation Microsoft Excel files (*.xls or *.xlsx), are produced in *.tif image format, such *.tif images will display hidden rows, columns, and worksheets, if any, in such files. The produced images shall reflect the native files as they were processed, including the files' settings as they were saved to the file before upload. Native files for all file extensions, with the exception of email messages, are to be included in the production, allowing the receiving party to view and/or download the native files for identification of any hidden data, tracked changes, comments or notes.

A.6. Parent-Child Relationships. Parent-child relationships (e.g., the associations between emails and their attachments) will be preserved. Email and other ESI attachments will be produced as independent files immediately following the parent email or ESI record. Parent-child relationships will be identified in the data load file pursuant to paragraph A.13 below.

A.7. Dynamic Fields. Files containing dynamic fields such as file names, dates, and times will be produced showing the field type (e.g., "[FILENAME]" or "[AUTODATE]"), rather than the values for such fields existing at the time the file is processed. The produced images shall reflect the native files as they were processed, including the files' settings as they were saved to the file before upload. Native files for all file extensions, with the exception of email messages, are to be included in the production, allowing the receiving party to view and/or download the native files for identification of any hidden data, tracked changes, comments or notes.

A.8. English Language. To the extent any data exists in more than one language, the data will be produced in English, if available. If no English version of a file is available, the Producing Party shall not have an obligation to produce an English translation of the data.

A.9. Embedded Objects. Some Microsoft Office and .RTF files may contain embedded objects. Such objects typically are the following file types: Microsoft Excel, Word, PowerPoint, Project, Outlook, and Access; and PDF. Subject to claims of privilege and immunity, as applicable, objects with those identified file types shall be extracted as separate files and shall be produced as attachments to the file in which they were embedded.

A.10. Compressed Files. Compressed file types (i.e., .CAB, .GZ, .TAR. .Z, .ZIP) shall be decompressed in a reiterative manner to ensure that a zip within a zip is decompressed into the lowest possible compression resulting in individual files.

A.11. Scanned Hardcopy Documents.

a. In scanning hardcopy documents, multiple distinct documents should not be merged into a single record, and single documents should not be split into multiple records (i.e., hard copy documents should be logically or physically unitized).

b. For scanned images of hard copy documents, OCR should be performed on a document level and provided in document-level *.txt files named to match the production number of the first page of the document to which the OCR text corresponds. OCR text should not be delivered in the data load file or any other delimited text file.

c. In the case of an organized compilation of separate hardcopy documents—for example, a binder containing several separate documents behind numbered tabs—the document behind each tab should be scanned separately, but the relationship among the documents in the binder should be reflected in proper coding of the family fields set out below.

A.12. Production Numbering. In following the requirements of Paragraph A.1, the Producing Party shall take reasonable steps to ensure that attachments to documents or electronic

files are assigned production numbers that directly follow the production numbers on the documents or files to which they were attached. If a production number or set of production numbers is skipped, the skipped number or set of numbers will be noted. In addition, wherever possible, each *.tif image will have its assigned production number electronically "burned" onto the image.

A.13. Data and Image Load Files.

a. Load Files Required. Unless otherwise agreed, each production will include a data load file in Concordance (*.dat) format and an image load file in Opticon (*.opt) format.

b. Load File Formats.

i. Load file names should contain the volume name of the production media. Additional descriptive information may be provided after the volume name. For example, both ABC001.dat or ABC001_metadata.dat would be acceptable.

ii. Unless other delimiters are specified, any fielded data provided in a load file should use Concordance default delimiters. Semicolon (;) should be used as multi-entry separator.

iii. Any delimited text file containing fielded data should contain in the first line a list of the fields provided in the order in which they are organized in the file.

c. Fields to be Included in Data Load File. For all documents or electronic files identified as relevant, not privileged, and produced, the following metadata fields for each document or electronic file, if available at the time of collection and processing and

unless such metadata fields are protected from disclosure by attorney-client privilege or work-product immunity or otherwise prohibited from disclosure by law or regulation, will be provided in the data load file pursuant to subparagraph (a). The term "Scanned Docs" refers to documents that are in hard copy form at the time of collection and have been scanned into *.tif images. The term "Email and E-Docs" refers to files that are in electronic form at the time of their collection, irrespective of the form (PDF-Plus, TIFF-Plus or native format) in which they are produced.

Field	Sample Data	Scanned Docs	Email and E-Docs	Comment
PRODBEG [Key Value]	ABC00000001	Yes	Yes	Beginning production number
PRODEND	ABC00000008	Yes	Yes	Ending production number
PRODBEGATT	ABC00000009	Yes	Yes	Beginning production number of parent in a family
PRODENDATT	ABC00001005	Yes	Yes	Ending production number of last page of the last attachment in a family
CUSTODIAN	Smith, John	Yes	Yes	Custodian(s) that possessed the document or electronic file—multiple custodians separated by semicolon
OTHER_CUSTODIANS	Doe, Jane; Jones, James	N/A	Yes	When global de-duplication is used, these are custodians whose file has been de-duplicated
NATIVEFILE	Natives\001\001\ABC 00000001.xls	N/A	Yes	Path and file name for native file on production media
FILEDESC	Microsoft Office 2007 Document	N/A	Yes	Description of the type file for the produced record.

Field	Sample Data	Scanned Docs	Email and E-Docs	Comment
FOLDER	\My Documents\Document1.doc	N/A	Yes	Original source folder for the record produced.
FILENAME	Document1.doc	N/A	Yes	Name of original electronic file as collected.
DOCEXT	DOC	N/A	Yes	File extension for email or e-doc
PAGES	2	Yes	Yes	Number of pages in the produced document or electronic file (not applicable to native file productions).
AUTHOR	John Smith	N/A	Yes	Author information as derived from the properties of the document.
DATECREATED	10/09/2005	N/A	Yes	Date that non-email file was created as extracted from file system metadata
DATELASTMOD	10/09/2005	N/A	Yes	Date that non-email file was modified as extracted from file system metadata
SUBJECT	Changes to Access Database	N/A	Yes	"Subject" field extracted from email message or metadata properties of the document
FROM	John Beech	N/A	Yes	"From" field extracted from email message
TO	Janice Birch	N/A	Yes	"To" field extracted from email message
CC	Frank Maple	N/A	Yes	"Cc" or "carbon copy" field extracted from email message
BCC	John Oakwood	N/A	Yes	"Bcc" or "blind carbon copy" field extracted from email message

Field	Sample Data	Scanned Docs	Email and E-Docs	Comment
DATESENT	10/10/2005	N/A	Yes	Sent date of email message (mm/dd/yyyy format)
TIMESENT	10:33 am	N/A	Yes	Sent time of email message, time zone set to GMT
DATERCVD	10/10/2005	N/A	Yes	Received date of email message (mm/dd/yyyyformat)
TIMERCVD	10:33 am	N/A	Yes	Received time of email message, time zone set to GMT
CONFIDENTIALITY	HIGHLY CONFIDENTIAL	Yes	Yes	Text of confidentiality designation, if any
TEXTPATH	Text\001\001\ABC00000001.txt	Yes	Yes	Path to *.txt file containing extracted or OCR text
FILE_PRODUCED_IN_NATIVE_AND_TIFF/PDF	Yes	N/A	Yes	Limited to documents reproduced in native format
MD5_HASH	309997447f.....	N/A	Yes	MD5 Hash value for ESI
PRODVOL	VOL001	Yes	Yes	Name of the Production Volume

A.14. Files Produced in Native Format.

a. For any electronic file produced initially as a native file in accordance with Paragraph B.2 of the Protocol above, the file shall be given a file name consisting of a unique Bates number and, as applicable, a suitable confidentiality designation; for example, "ABC00000002_Confidential." For each such native file, the production will include a *.tif image slipsheet (i) indicating the production number of the native file, (ii) with respect to any confidential document, setting forth the full confidentiality language applicable to the native file as set out in the protective order, and (iii) stating "File Provided Natively." To the extent that it is available, the original or redacted file

text shall be provided in a file-level multi-page UTF-8 text file with a text path provided in the *.dat file; otherwise the text contained on the slipsheet shall be provided in the *.txt file with the text path provided in the *.dat file.

b. For any electronic file produced in native file format following production of a PDF or TIFF-image in accordance with Paragraph B.1, the file shall be given a file name consisting of (i) the Bates number of the first page of the associated PDF or TIFF-image and (ii) as applicable, a suitable confidentiality designation. For each such native file, the production will include a new .DAT file (i) indicating the production number of the native file, (ii) identifying the path to the native file, (iii) adding a field stating "Yes," indicating that the file was produced in both native and PDF or TIFF formats, and (iv) linking the metadata associated with the originally produced PDF or TIFF image to the newly produced native file.

A.15. Production Media. Unless otherwise agreed, documents and ESI will be produced on optical media (CD/DVD), external hard drive, secure FTP site, or similar electronic format. Such media should have an alphanumeric volume name; if a hard drive contains multiple volumes, each volume should be contained in an appropriately named folder at the root of the drive. Volumes should be numbered consecutively (ABC001, ABC002, etc.). Deliverable media should be labeled with the name of this action, the identity of the Producing Party, and the following information: volume name, production range(s), and date of delivery.

A.16. Encryption of Production Media. To maximize the security of information in transit, any media on which documents or electronic files are produced may be encrypted by the Producing Party. In such cases, the Producing Party shall transmit the encryption key or password to the Requesting Party, under separate cover, contemporaneously with sending the

encrypted media. The Receiving Parties in this matter are on notice that certain data produced may originate from custodians in the European Union and the Receiving Parties therefore agree to follow the strictest security standards in guarding access to said data.